UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/933,760	08/22/2001	Timothy C. Williams	P62141US1	6977

136 7590 02/15/2005

JACOBSON HOLMAN PLLC
400 SEVENTH STREET N.W.
SUITE 600
WASHINGTON, DC 20004

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 02/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/933,760	WILLIAMS, TIMOTHY C.	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 December 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *25-32,34,37-45,47,49,54,59,69-71,73-75 and 85-89* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *25-32,34,37-45,47,49,54,59,69-71,73-75 and 85-89* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 25-32, 34, 37-45, 47, 49, 54, 59, 69-71, 73-75, and 85-89 have been examined. Applicant in the amendment filed on November 16, 2005 amended claims 25, 38, 54 and 69. Claims 1-24, 35-36, 48, 50-53, 55-58, 60-68, 72, and 76-84 were canceled in a previous amendment.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on November 16, 2004 has been entered.

Response to Arguments

3. Applicant's arguments with respect to amended claims 25-32, 34, 37-45, 47, 49, 54, 59, 69-71, and 73-75 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 25-27, 31, 34, 37-40, 44, 47, 49, 59, 69, 70-71, 74, and 85-87 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boyle et al. U.S. Patent No. 5,577,209 (hereinafter Boyle) in view of Chiniwala et al U.S. Patent No. 6,175,622 (hereinafter Chiniwala).

6. As per claim 25, Boyle discloses a multi-level secure network having a plurality of host computers accessible to users and connected to a network medium that has access to an untrusted line (see Boyle, Abstract; col. 2:46-65), the secure network comprising:

a. a network security controller for generating a user profile for each user and for sending the user profile to security devices connected to the network medium, the user profile defining at least one of a plurality of destinations which the user is authorized to access through discretionary access control and mandatory access control security mechanisms, wherein a plurality of user profiles define virtual private networks of communication comprising subsets of host computers (see Boyle, 3:30-42; 4:27-30 and 45-53; 5:33-65, especially lines

50-52; 6:15-32; 8:51-62, especially line 59; 9:38-46; 10:34-42; Figure 1 and related text); and

b. security devices connected to the network medium for receiving the user profiles generated at the network security controller and for implementing security mechanisms associated with the user profiles, each security device associated with one host computer, each security device having an authorization device for authorizing users at the associated host computer, the security device permitting the authorized user, via the associated host computer, to select a user's profile associated with the user and for restricting access of the host computer to the destinations defined in the selected user's profile (see Boyle, 5:1-8; 7:46-8:21, especially lines 47 and 51-52; 10:31-42; Figures 1, 4A-F, and 6A).

7. Boyle does not expressly disclose the network security controller generates a plurality of user profiles for a single user, wherein a single user selects a profile from the plurality of user profiles to access the restricted destinations. Chiniwala teaches generating a plurality of user profiles for a single user, wherein a single user selects a profile from the plurality of user profiles to access restricted destinations. See Chiniwala, col. 11:30-50; 12:16-19. Further, although Chiniwala discloses VPN as defined within the context of a telephony network whereas the VPN of Boyle is defined within the context of a computing network, the VPN described by Chiniwala corresponds to the functions and endusers of the VPN of Boyle. See Chiniwala, 4:12-16; Figure 1, Reference Nos. 34 and 26. Hence, it would be obvious to one of ordinary skill in the art

at the time the invention was made to apply the teaching of Chiniwala to the network disclosed by Boyle. Motivation to combine enables a single user to chose between multiple roles as taught by Chiniwala, ibid. The aforementioned covers the limitations of claim 25.

8. As per claim 26, the rejection of claim 25 is incorporated herein. In addition, the at least one destination comprises at least one other host computer of the network or the untrusted line. See Boyle, Figure 2, 'Bridge (SNIU)' and 'Gateway (SNIU)'; col. 5:50-53; 6:15-20.

9. As per claim 27, the rejection of claim 25 is incorporated herein. In addition, the security devices, when implementing security mechanisms, allows the host computer to connect to a trusted destination. See Boyle, col. 10:30-59.

10. As per claim 31, the rejection of claim 25 is incorporated herein. In addition, a user is prevented from simultaneously connecting to destinations having different security levels. See Boyle, col. 6:15-19.

11. As per claim 34, the rejection of claim 25 is incorporated herein. Although Boyle discloses that the network security measures of the invention are implemented at the session layer, Boyle also teaches end-to-end encryption devices conventionally operate at the network layer. See Boyle, col. 2:25-36. Moreover, the invention disclosed by

Boyle implements a sealer for encryption and decryption of data for secure transmission and integrity checks. See Boyle, Figure 4A, 'Sealer' and related text. It would be obvious to one of ordinary skill in the art at the time the invention was made to implement security at a network layer of protocol hierarchy. Motivation to combine enables the invention disclosed by Boyle to provide security services at the network layer and hence provide secure services without having to process the data at higher layers of the hierarchy as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 34.

12. As per claim 37, the rejection of claim 25 is incorporated herein. In addition, the security devices are integrated with the associated host computer. See Boyle, col. 11:24-26.

13. As per claims 38-40, and 44, they are method claims corresponding to claims 25-27, and 31 and they do not teach or define above the information claimed in claims 25-27, and 31. Therefore, claims 38-40, and 44 are rejected as being unpatentable over Boyle in view of Chiniwala for the same reasons set forth in the rejections of claims 25-27, and 31.

14. As per claim 47, it is a method claim corresponding to claims 34 and 38 and it does not teach or define above the information claimed in claims 34 and 38. Therefore,

claim 47 is rejected under Boyle in view of Chiniwala for the same reasons set forth in the rejections of claims 34 and 38.

15. As per claim 49, the rejection of claim 38 is incorporated herein. In addition, the destination in a user's profile corresponds to a level of security granted to the user. See Boyle, col. 4:60-65; 6:15-19; 9:38-46.

16. As per claim 59, the rejection of claim 25 is incorporated herein. Boyle discloses a means to update access control information by the network security controller, but does not specify updating user profiles at the network security controller and sending the updated user profiles to the security devices. See Boyle, col. 3:37-39; 10:35-37. However, as mentioned above, Boyle does disclose the secure network is divided into two roles: the security devices implement access control based on policies including discretionary rules, and the network security controller manages configuration management and security administration for the secure network. See Boyle, 4:27-30, 45-49; 5:1-7. Furthermore, Boyle teaches discretionary access rules are based on user identity. See Boyle, 5:40-45. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the network covered by Boyle to further comprise the steps of changing user profiles at the network security controller and updating available user profiles at a security device. Motivation to combine enables the method to perform updates to user profiles at the controller for centralized management

of access control to all devices in the secure network, and thus synchronizing changes to the secure network. The aforementioned cover the limitations of claim 59.

17. As per claim 69, the rejection of claim 25 is incorporated herein. In addition, Boyle discloses an embodiment of the invention wherein the security devices are implemented for internetwork connections (routing determination), and hence the security mechanisms to determine whether communication is authorized are implemented at a network layer of ISO protocol hierarchy. See Boyle, Figure 2, 'Gateway (SINU)' and 'Bridge (SINU)' and related text. Furthermore, if a receiving computer is not in a transmit list and/or is not consistent with a transmit window by means of discretionary and mandatory access controls, the transmission of information is terminated, otherwise the security device encrypts the information and transmits the encrypted information to the security device of the receiving computer over the computer network. See Boyle, col. 10:30-11:2; 5:33-65; 7:43-67. The aforementioned cover the limitations of claim 69.

18. As per claim 70, it is a method claim corresponding to the invention covered in the claim 59 and 69 rejections and it does not teach or define above the information in the invention covered in the claim 59 and 69 rejections. Therefore, claim 70 is rejected under Boyle in view of Chiniwala for the same reasons set forth in the rejections of claims 59 and 69.

19. As per claim 71, the rejection of claim 69 is incorporated herein. In addition, the method further comprises the step of auditing the termination of transmission of information at the network security controller. See Boyle, col. 6:34-39; 10:39-42; 3:15-21.

20. As per claim 74, the rejection of claim 69 is incorporated herein. In addition, the security device prevents simultaneous connection at different security levels established by mandatory access controls. See Boyle, col. 6:7-19; 5:54-65.

21. As per claim 85-87, the rejection of claim 25 is incorporated herein. In addition, the security devices include means for enabling a plurality of user profiles to be set for a single user (see Boyle, col. 3:30-42; see Chiniwala, 11:31-35), the plurality of user profiles to be set for a single user is specific to a particular host computer associated with the security device (see Boyle, 8:56-9:4; 9:35-45; see Chiniwala, 12:16-19), and at least one of the plurality of user profiles enables access to a plurality of destinations (see arguments to claim 25 rejection). The aforementioned cover the limitations of claims 85-87.

22. Claims 28-30, 41-43, 54, 73, 75, and 88-89 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boyle in view of Chiniwala, and further in view of Holden et al. U.S. Patent No. 5,828,832 (hereinafter Holden).

23. As per claim 28, the rejection of claim 25 is incorporated herein. Boyle does not expressly disclose alternative implementations of the invention wherein the host computer connects to an untrusted destination. Holden discloses a mixed enclave operation in a computer network with multi-level network security wherein the security device is configured to exploit this flexibility of mixed enclave operations. See Holden, col. 10:59-60. One configuration disclosed by Holden enables a host computer to connect to an untrusted destination wherein the security device does not implement security mechanisms. See Holden, 10:64-67. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Holden to the invention of Boyle. Motivation to combine enables a greater degree of flexibility with secure network host composition, since this configuration enables secure hosts to communicate with unsecured hosts and still offer a level of protection. See Holden, 11:2-5. The aforementioned cover the limitations of claim 28.

24. As per claim 29, the rejection of claim 28 is incorporated herein. In addition, the untrusted line comprises the Internet. See Boyle, Figure 1; see Holden, Figure 1, Reference No. 36.

25. As per claim 30, the rejection of claim 28 is incorporated herein. In addition, Holden discloses an implementation of the invention wherein a user cannot simultaneously communicate with a trusted destination and an untrusted destination. See Holden, col. 10:60-63.

26. As per claims 41-43, they are method claims corresponding to claims 28-30 and 38, and they do not teach or define above the information claimed in claims 28-30 and 38. Therefore, claims 41-43 are rejected under Boyle in view of Chiniwala and Holden for the same reasons set forth in the rejections of claims 28-30 and 38.

27. As per claim 54, the rejection of claim 29 is incorporated herein. In addition, the network security controller enables a security officer to generate the plurality of user profiles. See Boyle, col. 3:30-42. Further, data storage devices for temporarily storing data provided by a host computer are inherent features in data processing devices having functions outlined by Boyle. See Boyle, 7:43-56. Finally, Boyle discloses a means for transferring data out of the memory space while making the transferred data inaccessible to the host computer. See Boyle, Figures 3A-C; 2:46-54; 3:3-12; 4:40-44. The aforementioned cover the limitations of claim 54.

28. As per claims 73 and 75, they are method claims corresponding to claims 29-30 and 69 and they do not teach or define above the information claimed in claims 29-30 and 69. Therefore, claims 73 and 75 are rejected under Boyle in view of Chiniwala and Holden for the same reasons set forth in the rejections of claims 29-30 and 69.

29. As per claims 88 and 89, the rejection of claim 54 is incorporated herein. In addition, at least one of the plurality of user profiles includes a plurality of destinations

(see argument of claim 54), and the network security controller enables the security officer to generate different user profiles at different security devices for a single user. See Boyle, col. 3:30-42; 8:56-9:4; 9:35-45; see Chiniwala, 11:30-50.

30. Claims 32 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boyle in view of Chiniwala, and further in view of Stallings Cryptography and Network Security 2nd Edition (hereinafter Stallings).

31. As per claim 32, the rejection of claim 25 is incorporated herein. Boyle does not disclose a user only selecting one profile during a given connection establishment. However, the feature of mapping a user to a single profile at a given time is equivalent to a user securely logging into an account of a secure network. Stallings teaches a feature of the Kerberos authentication service wherein users are authenticated once per session. See Stallings, Figure 11.1. By enforcing a policy of mapping a single user to a single profile, user identification and accountability is more readily enforced. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention disclosed by Boyle to only allow a user to select one profile at a time. Motivation to combine enforces a more stringent network connection accountability. The aforementioned cover the limitations of claim 32.

32. As per claim 45, it is a method claim corresponding to claims 32 and 38 and it does not teach or define above the information claimed in claims 32 and 38. Therefore,

claim 45 is rejected under Boyle in view of Chiniwala and Stallings for the same reasons set forth in the rejections of claims 32 and 38.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Hagemann U.S. Patent No. 6,603,843 discloses defining a plurality of user profiles to access a virtual private network.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
February 10, 2005

GILBERTO BARRON SR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100